# 适用于多密级环境的移动存储设备互认证与密钥协商协议 *

冯　力[1]，郁　滨[1]，龚　碧[2]，周伟伟[1]

(1. 信息工程大学，郑州 450004; 2. 中国人民解放军 65012 部队，沈阳 110100)

**摘　要：** 针对多密级环境特点，提出一个能够离线认证、可识别密级的移动存储设备、主机终端互认证与密钥协商协议。协议基于 TTP（trusted third party）的数字签名不可伪造特性和计算离散对数问题(discrete logarithm problem)的困难性，通过验证协商密钥加密所得密文的正确性实现移动存储设备和主机终端的互认证。对协议进行非形式化和形式化分析，分析结果表明与同类协议相比，协议安全性较高，存储开销小，预共享认证参数次数少，实用性强。协议能够有效解决多密级环境下移动存储设备密级识别、身份认证问题，对移动存储设备安全管理具有重要意义。

**关键词：** 互认证；移动存储设备；多密级；SVO 逻辑

**中图分类号：** TP309.2　　doi: 10.3969/j.issn.1001-3695.2017.11.1003

# Mutual authentication and key negotiation protocol for removable storage devices applicable to multi-level environment

Feng Li[1], Yu Bin[1], Gong Bi[2], Zhou Weiwei[1]

(1. *Information Engineering University*, *Zhengzhou* 450004, *China*; 2. *PLA* 65012 *Troops*, *Shenyang* 110100, *China*)

**Abstract:** Considering the characteristics of multi-level environment, this paper proposes a mutual authentication and key negotiation protocol between removable storage devices and host terminals. There is no online authentication center and the protocol can be able to identify the confidentiality level. Based on the unforgeability of the digital signature from TTP (Trusted Third Party) and the difficulty of calculating the DLP (Discrete Logarithm Problem) , the protocol achieves mutual authentication between removable storage devices and host terminals through verifying the correctness of ciphertext encrypted by the negotiation key. Informal and formal analyses are put on the protocol. The analysis results show that the protocol has high security, small storage cost, low number of pre-shared authentication parameters and strong practicability compared with the similar protocols. This protocol can effectively solve the problem of confidentiality level identification and identity authentication of removable storage devices in multi-level environment. And it's of great importance to the security management of removable storage devices.

**Key Words:** mutual authentication; removable storage device; multi-level; SVO logic



## 0　引言

USB（universal serial bus）移动存储设备[1]因其使用方便、通用性好等优点广泛应用于数据存储与信息交互场合。然而由于缺乏必要的安全机制，USB 移动存储设备成为信息泄露的重要渠道[2-4]。特别是在多密级环境中，不同密级的信息系统通常采用物理隔离保证信息安全，而移动存储设备能轻易地打破安全边界，造成泄密[5]。因此需要对移动存储设备采取有效的技术手段进行管控，对其进行身份认证是实现管控的前提和基础[6]。

USB 移动存储设备认证协议可按有无在线认证中心分为两类，其中有在线认证中心的认证协议采用 C/S 模式，通过在线的认证服务器与客户端通信实现认证。Yang 等[7]首先提出一种基于 Schnorr 数字签名方案的移动存储设备认证协议，实现了用户和认证服务器互认证。Chen 等人[8]分析了文献[7]方案的弱点，提出了改进方案。Lee 等人[9]认为文献[8]的方案计算效率低，进而提出一种基于 ECC 的以用户口令、指纹、智能卡作为认证因子的三因子认证协议。He 等人[10]分析出文献[9]有容易遭到重放攻击等弱点，基于此进行了安全性改进。Giri 等人[11]提出一种基于用户指纹和口令的互认证方案，提高了指纹认证的安全性。文献[12]提出一种用于创建三因子安全协议的系统架构，提高了认证的效率，减少了通信和计算开销。Amin

**基金项目：** 国防重点实验室开放基金资助项目（KJ-14-103）

**作者简介：** 冯力（1992-），男，四川巴中人，硕士研究生，主要研究方向为信息安全、移动存储（291216217@qq.com）；郁滨（1964-），男，教授，博导，主要研究方向为信息安全、视觉密码；龚碧（1992-），男，助理工程师，硕士，主要研究方向为信息安全、移动存储；周伟伟（1990-），男，博士研究生，主要研究方向为信息安全、无线传感器网络.

等人[13]提出一种互认证和密钥协商协议，该协议仅通过注册服务器提供存储在设备上的机密信息的授权访问。上述协议利用在线的认证服务器对用户进行认证，未考虑设备和主机终端的合法性。由于多密级环境下不同密级终端相互隔离，无法建立在线的认证中心；并且攻击者可能使用伪造的设备或终端进行攻击，需要对其身份进行认证；因而此类协议只适用于网络互联的单一密级环境，无法满足多密级环境中移动存储设备认证需求。

无在线认证中心的协议通常基于预共享密钥、秘密参数、身份证书等方式实现移动存储设备与主机终端的身份认证。其中文献[14]实现了主机终端对移动存储设备的单向认证，但因未对主机终端认证，无法阻止非法主机访问移动存储设备。文献[15]提出一种基于 ECC 的 USB 认证密钥协商协议 UAKA，实现了 USB 移动存储设备与终端的互认证，但该协议无法抵抗中间人攻击。文献[16]通过共享认证因子实现 USB 设备与主机的双向认证，但该协议并不区分设备和主机的硬件特征，容易遭受介质伪造攻击。文献[17]提出一种基于安全芯片的可信移动存储设备的认证机制实现互认证。文献[18]利用混合密码体制设计能够识别安全等级的双向认证方案。然而由于文献[17,18]预共享的认证参数与主机终端身份有关，导致存储开销与主机终端数量成正比，且移动存储设备需要分别与所有终端一一预共享认证参数，不适用于终端数量较多的情形。文献[19]设计了一种用无线认证终端授权认证 U 盘的方法，由于需要引入新设备，提高了生产成本和管理成本。

本文旨在针对多密级环境的特点，设计一个无在线认证中心，可以识别密级的移动存储设备、主机终端互认证与密钥协商协议,从而有效地解决多密级环境中移动存储设备密级识别、身份认证问题。

# 1　预备知识

## 1.1　应用场景

多密级环境中，相同密级信息系统内信息可以自由传递，不同密级信息系统间物理隔离，信息只能从低密级向高密级传递。当使用移动存储设备在不同密级信息系统间交换数据时，由于其通用性和匿名性，移动存储设备能够破坏多密级环境中信息系统边界，极易导致信息无序地在信息系统间传递，造成泄密，如图 1 所示。

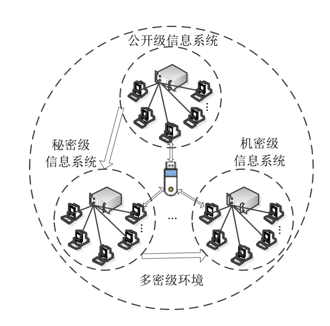



图 1　移动存储设备破坏安全边界示意图

针对上述问题，多密级环境下对移动存储设备的认证需要满足以下需求：a）能够标志移动存储设备密级，以确定其存储信息最高密级能力和传递数据的安全边界；b）能够标志主机终端密级，为确定主机访问移动存储设备权限提供依据，即主机对同密级的设备可读可写，对低密级设备只读；c）认证时无须认证服务器，能够离线认证；d）能够对主机和移动存储设备互认证，确保双向安全可靠。

## 1.2　总体结构

为方便描述，对协议使用到的符号及其含义进行说明，如表 1 所示。

表 1　协议符号说明表

| | |
|---|---|
| $D$：移动存储设备（简称设备） | $H$：主机终端（简称终端） |
| $UID_D$ :设备的唯一硬件特征 | $UID_H$：终端的唯一硬件特征 |
| $L_D$：设备分配的密级 | $L_H$：终端分配的密级 |
| $Cert(D)$：设备的证书 | $Cert(H)$：终端的证书 |
| $\bar{y}$：设备申请证书选取的秘密参数 | $\bar{x}$：终端申请证书选取的秘密参数 |
| $y$：设备认证时的新鲜因子 | $x$：终端认证时的新鲜因子 |
| $sk$：设备和终端协商的会话密钥 | T:可信第三方（TTP） |
| $K_t$ :可信第三方的公钥 | $K_t^{-1}$ 可信第三方的私钥 |
| $\{m\}_{K_t^{-1}}$：用私钥 $K_t^{-1}$ 对消息签名 | $\{m\}_{K_t}$：用公钥 $K_t$ 对证书进行验证签名 |
| $\{m\}_{sk}$：用密钥 $sk$ 对消息 $m$ 加密 | $\|$：连接符 |
| $\alpha$：$Z_p^*$ 的生成元 | $h(\bullet)$：哈希函数 |
| $p$：选取的大素数，$p \ge 2^{512}$，在 $Z_p^*$ 上计算离散对数问题是困难的 | |

协议的总体结构如图 2 所示。由管理部门根据实际需求将终端和设备划分为不同密级，密级用非负整数表示，密级越高，数字越大，密级相同，数字相等。TTP（Trusted Third Party）是权威、可信赖的第三方，是认证协议信任的源头，主要作用是为移动存储设备和主机终端发放密级标识。密级标识确定了移动存储设备（或主机终端）在多密级环境中存储信息的边界，即移动存储设备（或主机终端）所能存储信息的最高密级。对 TTP 的通信环境进行保护，因而信道可视为安全信道。攻击者的攻击手段有：窃听、阻止、截获、存储 USB 总线上的消息，发送消息给移动存储设备或主机终端。移动存储设备和终端通过在 USB 总线上运行认证协议，防止攻击者利用上述攻击手段使认证主体获得错误的密级。

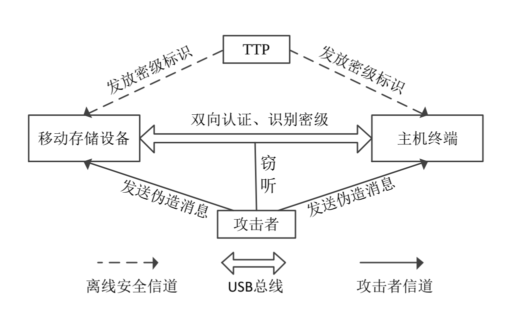



图 2　协议总体结构示意图

### 1.3 离散对数问题

离散对数问题可以描述为：给定一个素数 $p$ 和 $GF(p)$ 上的一个本原元 $\alpha$，对 $y \in GF(p)\backslash\{0\}$，找唯一的整数 $x$，$0 \le x \le p-2$，使得 $y = \alpha^x \bmod p$ 成立。一般的，如果仔细选择 $p$，那么认为该问题是困难的，即在计算上是不可行的。

## 2 协议设计

根据多密级环境下认证需求，对协议进行设计，协议分为初始化和互认证两个阶段。

### 2.1 协议初始化

协议初始化是指设备和终端申请证书，为实现互认证预共享认证参数的过程，初始化示意图如图 3 所示。

终端选择一个随机数 $\bar{x}$（$0 \le \bar{x} \le p-2$），并计算 $V_H = \alpha^{\bar{x}} (\bmod p)$，发送 $UID_H$、$V_H$ 至 TTP。TTP 为其分配密级 $L_H$，用自己私钥 $K_t^{-1}$ 签名，生成证书 $Cert(H)$ 并发送至终端，其中：

$$Cert(H) = L_H \| V_H \| \{h(UID_H \| L_H \| V_H)\}_{K_t^{-1}}$$

同样地，设备选择一个随机数 $\bar{y}$（$0 \le \bar{y} \le p-2$），并计算 $V_D = \alpha^{\bar{y}} (\bmod p)$，发送 $UID_D$、$V_D$ 至 TTP。TTP 为其分配密级 $L_D$，用自己私钥 $K_t^{-1}$ 签名，生成证书 $Cert(D)$ 并发送至设备，其中：

$$Cert(D) = L_D \| V_D \| \{h(UID_D, L_D, V_D)\}_{K_t^{-1}}$$

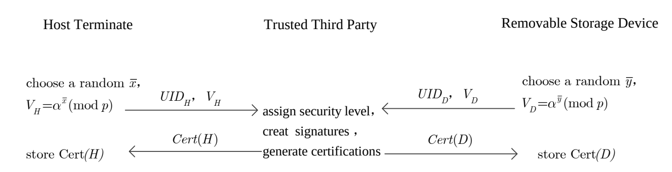


图 3 协议初始化示意图

### 2.2 互认证

互认证流程如图 4 所示。

a) 终端发起认证请求 REQ，选择一个随机整数 $x$ $(0 \le x \le p-2)$ 并计算 $\gamma_H = \alpha^x (\bmod p)$，将证书 $Cert(H)$、新鲜的临时值 $\gamma_H$ 和唯一硬件特征 $UID_H$ 发送至设备。

b) 设备计算 $\{\{h(UID_H \| L_H \| V_H)\}_{K_t^{-1}}\}_{K_t}$ 是否等于 $h(UID_H \| L_H \| V_H)$ 以验证证书 $Cert(H)$ 是否是 TTP 签发的合法证书，如果不是，协议终止，否则，协议转下一步。

c) 设备选择一个随机整数 $y$ $(0 \le y \le p-2)$ 并计算 $\gamma_D = \alpha^y (\bmod p)$，计算会话密钥 $sk = V_H^{\,y} \cdot \gamma_H^{\,\bar{y}} \bmod p$，并用会话密钥加密 $UID_D \| L_D \| \gamma_H \| \gamma_D$，将证书 $Cert(D)$、新鲜的临时值 $\gamma_D$、唯一硬件特征 $UID_D$ 和密文 $\{UID_D \| L_D \| \gamma_H \| \gamma_D\}_{sk}$ 发送至终端。

d) 终端计算 $\{\{h(UID_D, L_D, V_D)\}_{K_t^{-1}}\}_{K_t}$ 是否等于 $h(UID_D, L_D, V_D)$ 以验证证书 $Cert(D)$ 是否是 TTP 签发的合法证书，如果不是，协议终止，否则，协议转入下一步。

e)终端计算会话密钥 $sk = V_D^{\,x} \cdot \gamma_D^{\,\bar{x}} \bmod p$，并用会话密钥 $sk$ 加密 $UID_M \| L_M \| \gamma_C \| \gamma_M$ 得到 $\{UID_M \| L_M \| \gamma_C \| \gamma_M\}_{sk}$，如果与接收到的密文不一致，协议终止，否则，协议转入下一步。

f) 终端用会话密钥 $sk$ 加密 $UID_H \| L_H \| \gamma_D$，得到密文 $\{UID_H \| L_H \| \gamma_D\}_{sk}$，并发送至设备。

g)设备用会话密钥加密 $UID_H \| L_H \| \gamma_D$ 得到 $\{UID_H \| L_H \| \gamma_D\}_{sk}$，如果与接收到的密文不一致，认证失败、协议终止，否则，互认证通过。

需要说明的是，协议中可以采用任何一种计算上安全的签名和验证签名算法，签名和验证签名前须用散列函数对签名或验证签名内容进行散列。

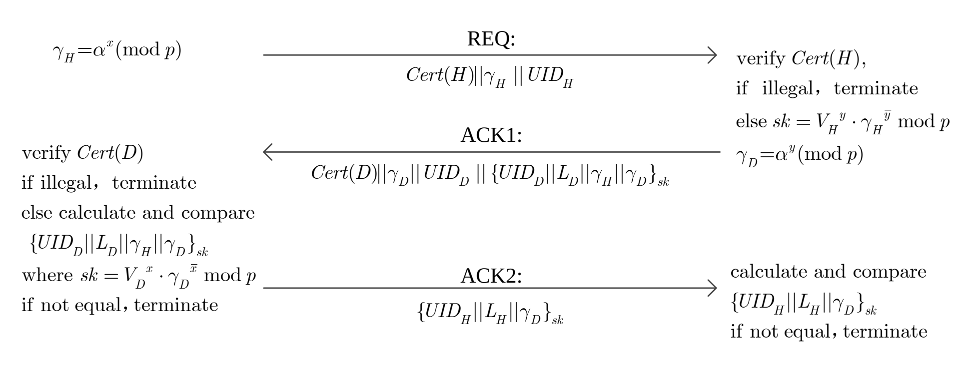


图 4 互认证流程示意图密钥协商

互认证通过后，终端获得协商密钥 $sk = V_D^{\,x} \cdot \gamma_D^{\,\bar{x}} \bmod p = \alpha^{\bar{x} \cdot y} \cdot \alpha^{x \cdot \bar{y}} \bmod p$，设备端获得协商密钥 $sk = V_H^{\,y} \cdot \gamma_H^{\,\bar{y}} \bmod p = \alpha^{\bar{x} \cdot y} \cdot \alpha^{x \cdot \bar{y}} \bmod p$，两者相等。因而双方可以使用协商密钥进行加密传输，保证 USB 总线上信息传输的安全。

## 3 协议性能效能分析

### 3.1 协议性能分析

协议基于 TTP 的数字签名不可伪造特性和计算离散对数问题的困难性，在认证过程中，随机产生的新鲜因子密文传送，具有较好的安全特性，分析如下：

1）抗介质伪造攻击（media forgery attack）

介质伪造攻击是指攻击者使用未认证的存储介质代替已认证的存储介质，通过更换存储介质的手段达到窃取秘密信息的目的。在协议初始化阶段，移动存储设备将唯一硬件信息（例如存储介质的全球唯一序列号 GUID）发送给 TTP，TTP 对包含上述信息的内容进行签名。认证时，移动存储设备须将唯一

硬件信息 $UID_D$ 发送至主机，如果攻击者更换介质，会导致当前介质 $UID_D'$ 与设备申请证书时的 $UID_D$ 不一致，从而主机在验证设备证书时不通过，因此协议可以抵抗介质伪造攻击。

2）抗盗窃证书攻击（stolen-verifier attack）

攻击者即使盗取了合法设备的证书也无法仿冒合法设备通过认证。这是因为每个证书与设备申请证书时的秘密参数 $\bar{y}$ 是一一对应的，攻击者仅仅盗窃合法设备的证书，只能通过互认证中第④步，即验证证书合法性的一步，然而由于攻击者无法得知设备的秘密参数 $\bar{y}$，也就无法计算出正确的会话密钥 $sk$，从而无法通过认证。类似地，攻击者即使盗取合法终端的证书，由于无法得知秘密参数 $\bar{x}$，也就无法计算正确的 $sk$，也就无法通过认证。综上，协议可以抵抗盗窃证书攻击。

3）抗重放攻击（replay attack）

协议采用挑战应答机制，在通信过程中，主机终端生成随机数 $x$，移动存储设备生成随机数 $y$ 作为新鲜因子，并将新鲜因子加密为 $\gamma_H$ 和 $\gamma_D$ 再传送。假设攻击者通过侦听信道可以获得信道上所有消息：REQ、ACK1、ACK2 并进行重放攻击，由于仅知道 $\gamma_H$ 或 $\gamma_D$，计算得到 $x$ 或 $y$ 是困难的，从而无法计算正确的会话密钥 $sk$，导致无法通过认证。同时由于每一回合生成的随机数都是新鲜的，因而攻击者也无法通过重放以往回合中侦听到的陈旧的消息实施重放攻击。

4）抗中间人攻击（man-in-the-middle attack）

通信双方通过协商会话密钥 $sk$，并利用 $sk$ 加密新鲜的临时值 $\gamma_D$、$\gamma_H$ 得到握手消息 ACK1、ACK2，通过独立地验证握手消息的正确性来确认对方身份。中间人仿冒终端或设备发起攻击时，由于没有秘密参数 $\bar{x}$ 或 $\bar{y}$，无法计算得到正确的会话密钥，也就无法加密临时值 $\gamma_D$、$\gamma_H$ 获得正确的密文，无法通过认证，因此攻击者无法作为中间人冒充合法设备或终端。

5）前向安全性（forward secrecy）

协议通过协商会话密钥 $sk = V_H{}^{y} \cdot \gamma_H{}^{\bar{y}} \bmod p = V_D{}^{x} \cdot \gamma_D{}^{\bar{x}} \bmod p$ 保护认证和通信安全，每一次认证，生成的临时值 $x$、$y$ 都是新鲜的，并且每一次会话密钥只在一次认证中使用，因而每一次认证的会话密钥都是不同的。即使攻击者获得了主机或设备的秘密参数，也无法计算出之前所生成的会话密钥，保证了前向安全性。

6）离线认证

认证时，只有设备和终端参与认证，无须在线的认证中心，适用于多密级环境下不同密级信息系统间物理隔离的情形。

7）可识别密级

为适应多密级环境，在协议初始化时，为设备和终端分配了密级标识。如果通过互认证，终端和设备都能获取对方可信的密级标志，从而识别密级，为访问控制奠定基础。

协议主要安全特性与相关文献对比如表 2 所示。

### 3.2 协议效能分析

设定 $UID_D$、$UID_H$ 为 80bit，$L_D$、$L_H$ 为 8 bit，公钥为 512 bit，私钥为 140 bit，公钥加密、签名结果为 1024 bit，哈希结果为 128 bit，随机数为 140bit，M 为多密级环境中主机终端数量,N 为移动存储设备数量。$T_{enc}/T_{dec}$ 表示一次对称加解密运算所需时间，$T_{penc}/T_{pdec}$ 表示一次公钥加解密运算所需时间，$T_{sig}/T_{ver}$ 表示一次签名或验证签名操作所需时间，$T_{hash}$ 表示一次散列运算所需时间，$T_{me}$ 表示一次模幂运算所需时间，$T_{xor}$ 表示一次异或运算所需时间。

文献[17，18]都采用了无在线认证中心的结构，应用领域与本文相同，与之进行对比分析。如表 3 所示，本文协议存储开销为 1764bit，优于文献[17，18]，原因在于文献[17，18]没有设立可信第三方，导致存储开销与终端数量成正比，当终端数量很大时，存储开销将变得难以接受。为保证环境中所有移动存储设备和主机终端能够互认证，文献[17，18]中移动存储设备需与主机终端一一预共享认证参数，共计 M*N 次，而本文协议只需 M+N 次，大大减少了预共享认证参数次数，实用性更强。

表 3 协议存储开销和预共享参数次数对比

| | 文献[17] | 文献[18] | 本文 |
|---|---|---|---|
| 存储开销（bit） | 1056*M | 1224*M | 1764 |
| 预共享认证参数次数 | M*N | M*N | M+N |

如表 4 所示，本文协议计算开销为 2 $T_{hash}$ +4 $T_{me}$ +2 $T_{ver}$ +4 $T_{enc}$，明显低于文献[17],与文献[18]持平，高于文献[11，12]。文献[11，12]虽然计算开销较小，但因采用认证服务器实现认证，不适用于多密级环境。

## 4 协议形式化分析

SVO 逻辑是目前分析认证协议最有力的形式化推理方法之一，应用 SVO 逻辑对提出的互认证协议进行形式化分析。

### 4.1 公理及规则

SVO 逻辑遵从两条推理规则和 20 条公理，将需要使用的列举如下：

MP 规则：由 $\psi$ 和 $\varphi \supset \psi$ 可以推出 $\psi$。

Nec 规则：由 $\vdash \varphi$ 可以推导出 $\vdash P \mid\equiv \varphi$。

$$A_1: P \mid\equiv \varphi \wedge P \mid\equiv (\varphi \supset \psi) \supset P \mid\equiv \psi$$

$$A_3: P \overset{K}{\longleftrightarrow} Q \wedge R \lhd \{X^Q\}_K \supset (Q \mid\sim X \wedge Q \ni K)$$

$$A_4: PK_\sigma(Q,K) \wedge R \lhd X \wedge SV(X,K,Y) \supset Q \mid\sim Y$$

$$A_5: PK_\delta(P,K_P) \wedge PK_\delta(Q,K_q) \supset P \overset{K_{pq}}{\longleftrightarrow} Q$$

$$A_7: P \lhd (X_1,\cdots,X_n) \supset P \lhd X_i$$

应用公理 $A_1$ 和 MP 规则，可以得到以下常用结论：

$$A_1 + MP: (P \mid\equiv \varphi \wedge P \mid\equiv (\varphi \supset \psi)) \vdash P \mid\equiv \psi)$$

### 4.2 初始假设集合

协议中的消息 $UID_D$、$L_D$ 是移动存储设备的待认证信息，用 D 表示，同样的，消息 $UID_H$、$L_H$ 用 H 表示。主机终端 H 的初始假设集合为：

$$P_1: H \mid\equiv PK_\sigma(T, K_t)$$

$$P_2: H \mid\equiv SV(\{D, V_D\}_{K_t^{-1}}, K_t, (D, V_D))$$

$$P_3: H \mid\equiv EV((D, \gamma_H, *d), sk, \{D, \gamma_H, *d\}_{sk})$$

$$P_4: H|\equiv((T|\sim PK_\delta(D,V_D)\wedge H\triangleleft((D,V_D),\{D,V_D\}_{K_t^{-1}},*d,\{D,\gamma_H,$$
$$*d\}_{sk})\wedge EV((D,\gamma_H,*d),sk,\{D,\gamma_H,*d\}_{sk}))\supset PK_\delta(D,(V_D,*d)))$$
$$P_5: H|\equiv PK_\delta(H,(V_H,\gamma_H))$$
$$P_6: H\triangleleft(D,V_D,\{D,V_D\}_{K_t^{-1}},\gamma_D,\{D,\gamma_H,\gamma_D\}_{sk})$$
$$P_7: H|\equiv H\triangleleft(D,V_D,\{D,V_D\}_{K_t^{-1}},*d,\{D,\gamma_H,*d\}_{sk})$$
$$P_8: H|\equiv(T|\sim(D,V_D)\supset T|\sim PK_\delta(D,V_D))$$

$P_1\sim P_5$ 反映了主机终端 H 的初始信念，其中 $P_1$ 表明 H 相信 $K_t$ 是可信第三方 T 的公开签名验证密钥；$P_2$ 表明 H 相信密钥 $K_t$ 可以验证 $\{D,V_D\}_{K_t^{-1}}$ 是 $(D,V_D)$ 的签名；$P_3$ 引入符号 $EV(X,K,Y)$ 表示用密钥 $K$ 加密 $X$ 得到 $Y$，即 $\{X\}_K=Y$，用于验证密钥的正确性，表明 H 相信 $sk$ 加密 $(D,\gamma_H,*d)$ 得到 $\{D,\gamma_H,*d\}_{sk}$；$P_4$ 表明 H 相信如果 T 发送过 $PK_\delta(D,V_d)$ 且 H 接收到消息：$((D,V_D),\{D,V_D\}_{K_t^{-1}},*d,(D,\gamma_H,*d)_{sk})\wedge EV((D,\gamma_H,*d),sk,(D,\gamma_H,*d)_{sk}))$，则 $V_D$、$*d$ 是设备 D 的公开协商参数。$P_5$ 表明 H 相信 $V_H$、$\gamma_H$ 是 H 的公开协商参数。$P_6$ 是接收消息，表明 H 接收到消息 $(D,V_D,\{D,V_D\}_{K_t^{-1}},\gamma_D,\{D,\gamma_H,\gamma_D\}_{sk})$。$P_7$ 是理解消息，表明 $\gamma_D$ 是 H 收到的不可识别的消息。$P_8$ 是解释消息，表明 H 相信如果 T 发送过 D、$V_D$，则 $V_D$ 是 D 的公开协商参数。对于移动存储设备的初始假设集合，除以下 2 条外，其余可以对称得到：

$$P_6': D\triangleleft(H,V_H,\{H,V_H\}_{K_t^{-1}},\gamma_H),\ D\triangleleft(\{H,\gamma_D\}_{sk})$$
$$P_7': D|\equiv D\triangleleft(H,V_H,\{H,V_H\}_{K_t^{-1}},*h)$$

表 2　协议安全特性对比

| | 文献[7] | 文献[9] | 文献[10] | 文献[11] | 文献[15] | 文献[16] | 文献[17] | 文献[18] | 本文 |
|---|---|---|---|---|---|---|---|---|---|
| 抗介质伪造攻击 | × | × | × | × | × | × | √ | × | √ |
| 抗重放攻击 | × | × | √ | √ | √ | √ | √ | √ | √ |
| 抗中间人攻击 | √ | √ | √ | √ | × | √ | √ | √ | √ |
| 离线认证 | × | × | × | × | √ | √ | √ | √ | √ |
| 可识别密级 | × | × | × | × | × | × | × | √ | √ |

表 4　协议计算开销对比

| | 协议初始化 | 认证 | | 总计 |
|---|---|---|---|---|
| | | 移动存储设备 | 主机终端 | |
| 文献[11] | $5T_{hash}+1T_{dec}$ | $1T_{hash}+1T_{me}$ | $4T_{hash}+1T_{me}$ | $10T_{hash}+2T_{me}+1T_{dec}$ |
| 文献[12] | $5T_{hash}+1T_{enc}$ | $2T_{hash}$ | $4T_{hash}+1T_{enc}$ | $11T_{hash}+2T_{enc}$ |
| 文献[17] | $2T_{me}$ | $2T_{sig}+2T_{penc}+1T_{pdec}+1T_{ver}+3T_{hash}$ | $2T_{pdec}+2T_{ver}+1T_{sig}+1T_{penc}+3T_{hash}$ | $6T_{hash}+3T_{sig}+3T_{ver}$ $+3T_{penc}+3T_{pdec}+2T_{me}$ |
| 文献[18] | $1T_{xor}+1T_{penc}$ | $1T_{penc}+1T_{pdec}+1T_{xor}+1T_{dec}+1T_{hash}$ | $1T_{penc}+1T_{pdec}+1T_{enc}+1T_{hash}$ | $2T_{hash}+3T_{penc}+2T_{pdec}+2T_{xor}+1T_{enc}+1T_{dec}$ |
| 本文 | $1T_{me}$ | $1T_{hash}+1T_{ver}+2T_{me}+2T_{enc}$ | $1T_{hash}+1T_{ver}+2T_{me}+2T_{enc}$ | $2T_{hash}+4T_{me}+2T_{ver}+4T_{enc}$ |

### 4.3　安全性证明

**假设 1**　第三方 T 是可信的，其数字签名方案是安全的，攻击者无法伪造其签名。

**假设 2**　求解离散对数问题是困难的，计算上不可行。

**结论 1**　如果证书是由第三方 T 签名，并且移动存储设备拥有秘密参数 $y$ 和 $\bar{y}$，那么可以唯一确认移动存储设备的合法身份。

协议通过验证移动存储设备证书的数字签名和协商密钥加密临时值所得密文的正确性确认移动存储设备身份合法性。如果通过验证签名算法计算得到移动存储设备的证书是第三方 T 签名，根据假设 1，由于攻击者无法伪造其签名，则可认定该证书是值得信任的。攻击者即使截获总线上可信的证书，为验证通过协商密钥加密临时值所得密文的正确性，攻击者必须获得协商密钥；由于协商密钥 $sk=V_C{}^{y}\cdot\gamma_C{}^{\bar{y}} \bmod p$，攻击者必须获得秘密参数 $y$ 和 $\bar{y}$；然而由于假设 2，根据总线上的消息 $\alpha^{\bar{y}}$ 或 $\alpha^{y}$，计算 $y$ 和 $\bar{y}$ 是困难的，攻击者无法仿冒，因此可以唯一确认移动存储设备的合法身份。

类似地，可以证明结论 2。

**结论 2**　如果证书由可信第三方签名，并且主机终端拥有秘密参数 $x$ 和 $\bar{x}$，那么可以唯一确认主机终端的合法身份。

根据结论 1、2，协议目标可用 SVO 逻辑表达为

$$H|\equiv T|\sim(D,V_D)\qquad H|\equiv D\ni(\bar{y},y)$$
$$D|\equiv T|\sim(H,V_H)\qquad D|\equiv H\ni(\bar{x},x)$$

形式化证明如下：

由 $A_7$ 和 Nec 规则可得：

$$H|\equiv(H\triangleleft(D,V_D,\{D,V_D\}_{K_t^{-1}},*d,\{D,\gamma_H,*d\}_{sk})\supset H|\equiv H\triangleleft(\{D,V_D\}_{K_t^{-1}}))\tag{1}$$

由 $P_7$ 和式（1），应用结论 $A_1+MP$ 可得：

$$H|\equiv(H\triangleleft(\{D,V_D\}_{K_t^{-1}}))\tag{2}$$

由 $P_1$、式（2）、$P_2$ 可得：

$$H|\equiv PK_\sigma(T,K_t)\wedge H\triangleleft(\{D,V_D\}_{K_t^{-1}})\wedge SV(\{D,V_D\}_{K_t^{-1}},K_t,(D,V_D))\tag{3}$$

将公理 $A_4$ 实例化，并应用 Nec 规则可得：

$$H|\equiv(PK_\sigma(T,K_t)\wedge H\triangleleft(\{D,V_D\}_{K_t^{-1}})\wedge SV(\{D,V_D\}_{K_t^{-1}},K_t,(D,V_D))$$
$$\supset T|\sim(D,V_D))\tag{4}$$

由式（3）（4），应用 $A_1+MP$ 可得：

$$H \mid\equiv T \mid\sim (D, V_D) \tag{5}$$

由式（5）和 $P_8$，应用 $A_1 + MP$ 可得：

$$H \mid\equiv T \mid\sim PK_\delta(H, V_H) \tag{6}$$

由式（6）、$P_7$、$P_3$ 可得：

$$H \mid\equiv T \mid\sim PK_\delta(D, V_D) \wedge H \triangleleft (D, V_D, \{D, V_D\}_{K_t^{-1}}, *d, \{D, \gamma_H, *d\}_{sk}$$
$$\wedge EV((D, \gamma_H, *d), sk, \{D, \gamma_H, *d\}_{sk}) \tag{7}$$

由式（7）、$P_4$，应用 $A_1 + MP$ 可得：

$$H \mid\equiv PK_\delta(D, (V_D, *d)) \tag{8}$$

由 $P_5$ 和式（8）可得：

$$H \mid\equiv (PK_\delta(H, (V_H, \gamma_H)) \wedge PK_\delta(D, (V_D, *d))) \tag{9}$$

将公理 $A_5$ 实例化，应用 Nec 规则可得：

$$H \mid\equiv (PK_\delta(H, (V_H, \gamma_H)) \wedge PK_\delta(D, (V_D, *d)) \supset H \xleftrightarrow{sk} D) \tag{10}$$

其中 $sk$ 如式（11）：

$$sk = F_0(V_H, \gamma_H, V_D, *d) = (V_D)^x \cdot (\gamma_D)^{\bar{x}} = (V_H)^y \cdot (\gamma_H)^{\bar{y}} = \alpha^{\bar{x}y + x\bar{y}} \tag{11}$$

由式（9）（10），应用 $A_1 + MP$ 可得：

$$H \mid\equiv H \xleftrightarrow{sk} D \tag{12}$$

由式（12）、$P_7$，将公理 $A_7$ 实例化，应用 Nec 规则和 $A_1 + MP$ 可得：

$$H \mid\equiv (H \xleftrightarrow{sk} D \wedge H \triangleleft \{D, \gamma_H, *d\}_{sk}) \tag{13}$$

由式（13），将公理 $A_3$ 实例化，应用 Nec 规则和 $A_1 + MP$ 可得：

$$H \mid\equiv (D \mid\sim (D, \gamma_H, *d) \wedge D \ni sk) \tag{14}$$

由式（14）可得：

$$H \mid\equiv D \ni sk \tag{15}$$

由式（15）、$sk$ 定义式（11）以及 $\bar{x}$、$\bar{y}$、$x$、$y$ 的定义可得：

$$H \mid\equiv D \ni (\bar{y}, y) \tag{16}$$

由式（5）（16）构成了主机终端的信念集合。

同样地，对移动存储设备 D 也可以做类似的分析，得到以下结果：

$$D \mid\equiv T \mid\sim (H, V_H) \tag{17}$$

$$D \mid\equiv H \ni (\bar{x}, x) \tag{18}$$

这一结果表明，协议能够达到预期目标：安全地实现主机终端和移动存储设备互认证。

## 5　结束语

在分析多密级环境特点基础上，提出了一个能够离线认证，可识别设备和终端密级的互认证与密钥协商协议。协议的安全性基于可信第三方数字签名不可伪造特性和计算离散对数问题的困难性，经过分析证明协议安全性较高，存储开销小，预共享认证参数次数少，实用性强，能够有效地解决多密级环境下移动存储设备的密级识别、安全认证问题，为其访问控制奠定安全基础。

## 参考文献：


[1] IEEE B E. 1667-2006 IEEE standard protocol for authentication in host attachments of transient storage devices [S]. 2010: 1-125.

[2] Pham D V, Syed A, Halgamuge M N. Universal serial bus based software attacks and protection solutions [J]. Digital Investigation, 2011, 7 (3–4): 172-184.

[3] 张慧敏. USB 存储设备安全机制的研究与实现 [D]. 成都: 电子科技大学, 2016.

[4] 吕志强, 刘喆, 常子敬, 等. 恶意 USB 设备攻击与防护技术研究 [J]. 信息安全研究, 2016, 2 (2): 150-158.

[5] 刘一. 对我军移动存储介质安全保密管理的思考 [J]. 信息安全与技术, 2012, 3 (10): 8-9.

[6] 赵松银, 郁滨. USB 安全连接方案设计与实现 [J]. 系统仿真学报, 2016 (6): 1400-1405.

[7] Yang F Y, Wu T D, Chiu S H. A secure control protocol for USB mass storage devices [J]. IEEE Trans on Consumer Electronics, 2011, 56 (4): 2239-2343.

[8] Chen B, Qin C, Yu L. A secure access authentication scheme for removable storage media [J]. Journal of Information & Computational Science, 2012. 9 (15): 4353-4363,

[9] Lee C C, Chen C T, Wu P H, et al. Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices [J]. Iet Computers & Digital Techniques, 2013, 7 (1): 48-56.

[10] He D, Kumar N, Lee J H, et al. Enhanced three-factor security protocol for consumer USB mass storage devices [J]. IEEE Trans on Consumer Electronics, 2014, 60 (1): 30-37.

[11] Giri D, Sherratt R S, Maitra T, et al. Efficient biometric and password based mutual authentication for consumer USB mass storage devices [J]. IEEE Trans on Consumer Electronics, 2016, 61 (4): 491-499.

[12] Giri D, Sherratt R S, Maitra T. A novel and efficient session spanning biometric and password based three-factor authentication protocol for consumer USB Mass Storage Devices [J]. IEEE Trans on Consumer Electronics, 2016, 62 (3): 283-291.

[13] Amin R, Sherratt R S, Giri D, et al. A software agent enabled biometric security algorithm for secure file access in consumer storage devices [J]. IEEE Trans on Consumer Electronics, 2017, 63 (1): 53-61.

[14] 王黎, 蔡皖东. 移动存储介质安全管理系统设计与实现 [J]. 信息安全与通信保密, 2007, 25 (2): 119-121.

[15] 杨先文, 李峥, 王安, 等. 密码安全 USB 设备控制器 IP 的系统设计 [J]. 华中科技大学学报: 自然科学版, 2010 (9): 59-62.

[16] 李翠, 郁滨. 一种具有身份认证功能的 USB IP 核设计与实现 [C]// 计算机技术与应用学术会议论文集. 2012: 580-585.

[17] 王冠, 李天亮. 一种基于安全芯片的可信移动存储设备的双向认证机制 [J]. 计算机与应用化学, 2013 (5): 15-18.

[18] 张学思, 基于移动存储设备的多密级安全交互系统设计与实现 [D]. 郑州: 信息工程大学, 2015.

[19] 丁贤根. 用无线认证终端授权认证及加解密的安全 U 盘设计方法: 中国, 103366797 B [P]. 2016.